Secure Internet Commerce -- Design and Implementation of the Security Architecture of Security First Network Bank, FSB.

Nicolas Hammond
NJH Security Consulting, Inc.
211 East Wesley Road
Atlanta, GA 30305-3774
Tel: 404-262-1633
Fax: 404-812-1984
njh@njh.com
http://www.njh.com

Abstract

Security First Network Bank (SFNB) (**http://www.sfnb.com**) went on-line in October 1995 as the world's first on-line bank. The paper discusses how the security architecture was designed and implemented using the most currently available security technologies.

The encryption technologies used to transport information across the Internet are widely known. Less widely known is how to protect the systems that are directly connected to the Internet, but must interact with customers and protect sensitive information.

This paper discusses the measures that were taken to ensure that SFNB is as safe as possible against hackers. Not only did the entire system have to be safe against attacks but the systems also needed to have the security and assurance needed to meet the Office of Thrift and Supervision approval.

Design Process

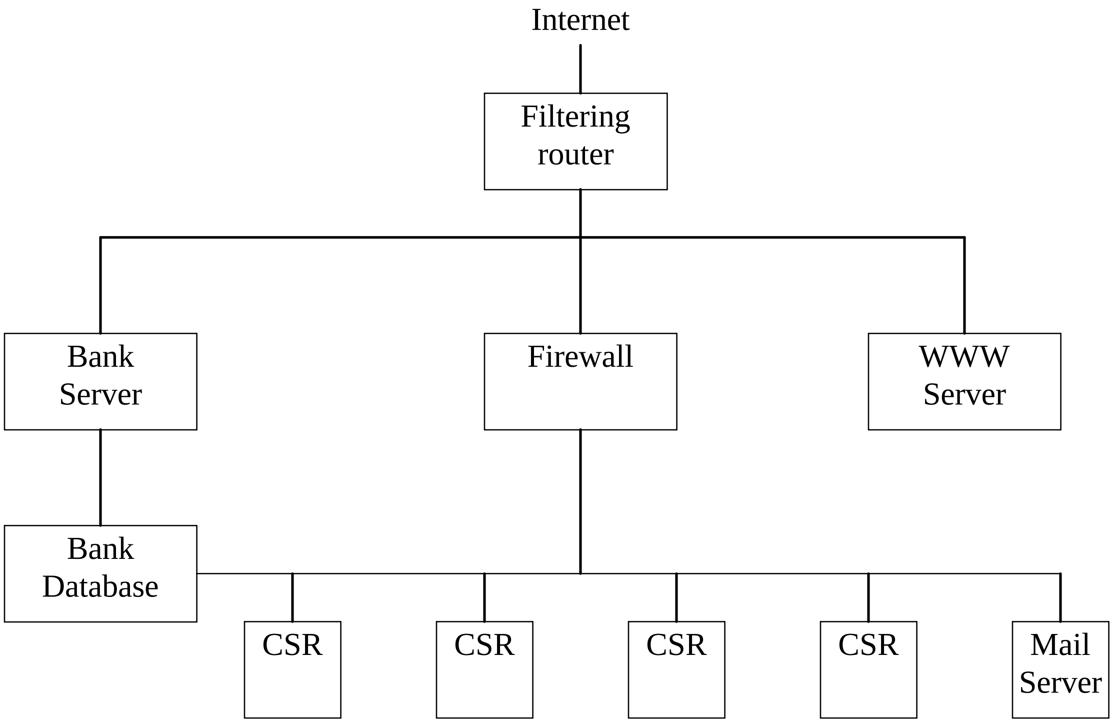
The design of the security architecture began in early 1995. A security architecture paper was written and reviewed by security experts. The design goals were to use sufficient security technology to protect all parts of the bank operations, but at the same time to create a system that could be easily administered by competent system administrators.

The main difference between protecting an on-line bank, and providing a firewall for a commercial company, is that the bank database must be accessible to outside users and therefore has to be protected by a much stronger machine than a conventional firewall. A large part of the architecture discussed how to protect this machine, what type of machine it should be, and the administrative controls that would be needed.

After thorough reviews, the architecture was approved and a security policy was written based upon the security architecture. The time taken to correctly design both the security architecture and the security policy was well spent as it has not been necessary to substantially change either.

Machine Architecture

The security of the entire system rests upon the security of every machine in that system. If a single machine is vulnerable, then potentially the whole network is vulnerable. One of the first stages of the overall design was understanding the data that would flow through the system. Careful consideration was then placed on what machines were needed, and how the machines would be connected.



Except for the Bank Server, this is a fairly typical commercial firewall implementation.

Filtering Router

The filtering router prevents IP-spoofing attacks by ensuring that no incoming packets have an “inside” address. The filtering router also implements filtering rules for each machine to ensure that only authorized traffic is sent to this machine. For example, the WWW server should only receive packets destined for TCP port 80 (http port), the Bank Server should only receive packets for TCP port 443 (https port). The filtering router logs all errors. These error logs have been an invaluable source of information.

WWW Server

The WWW server provides information on the bank to potential customers. The only port that is open on this machine is TCP port 80 (http port). All other network services are de-configured from this machine.

Firewall

The firewall is a dual-homed bastion host running a mail application proxy. Mail is the only traffic allowed to pass through the firewall to the internal network. The firewall also acts as the Domain Name Server (DNS) for the machines in the DMZ. The firewall selected was *Interceptor*, a firewall product from Technologic (**http://www.tlogic.com**).

Customer Service Representative (CSR) Network

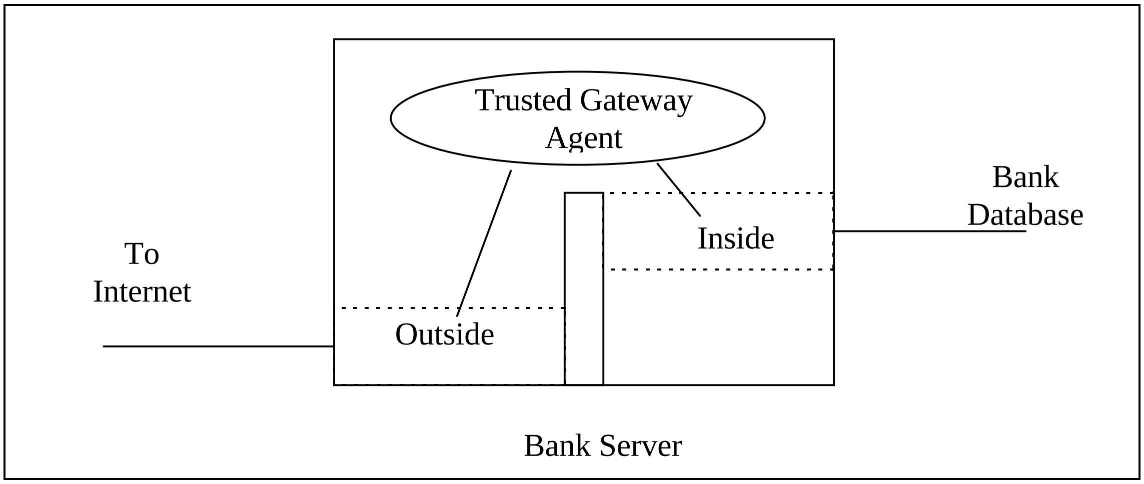
The CSR machines are on a dedicated network. Each CSR has a machine that can be used for receiving and sending mail (stored on a central mail server, external mail sent through the firewall). Each CSR also has read-only access to portions of the bank database to handle bank customer telephone queries. All database actions are audited and can be traced to an individual CSR if necessary.

Bank Database

The Bank Database is the heart of the bank's data center. The machine is dual-homed, with one network card connected to the CSR network to allow CSR read-only access to the database and the other network card connected to the Bank Server. Although all machines need to have a high availability, this machine also needs very high data integrity and so RAID disks are used.

Bank Server

The Bank Server is the machine that protects the bank database. Whereas most firewalls protect internal clients, this machine protects an internal server and therefore needs to be more secure than a firewall and have very strong assurances that it cannot be compromised. Because of these requirements, this machine uses the multilevel secure HP/UX CMW. All features of a trusted system are used -- least privilege, discretionary access control (DAC), mandatory access control (MAC), system integrity and audit.



The Bank Server is dual-homed. One network is connected to the "outside" and runs the Netscape Commerce Server to provide encrypted web traffic through the Secure Socket Layer (SSL). The other network card connects to the "inside" and the Bank Database. Because the "outside" and the "inside" need to be kept totally separate, this machine uses the multilevel capabilities of the HP/UX CMW and assigns a different category for each network. A small trusted program connects the Netscape Commerce Server (running at the "outside" level) with the actual bank applications that run at the "inside" level.

The use of different categories, “inside” and “outside”, provides very strong assurance to the system. Only the Netscape Commerce Server is listening on the “outside” network, all other network services are de-configured. The Netscape Commerce Server is running at the “outside” level. According to the HP/UX CMW rules, a process can only write to files at the same level. The only files at the “outside” level are the Netscape log files.

There are very few applications that make use of the *chroot* capability on Unix systems. One of the design features was to make as much use as possible of the underlying security mechanisms. Therefore, the Netscape Commerce Server runs in a *chroot-ed* environment that only contains the files needed to run it. Note, that the Netscape Commerce Server is started in a *chroot-ed* environment - this is different from using the *chroot* capability of a web server. Therefore, even if there was a bug in the Netscape Commerce Server that allowed an outside user to create a shell, this shell would be running in a *chroot-ed* environment with very few files in it, could only write to the Netscape log files, and is running at an “outside” level so could not even see any files or networks on the “inside."

A side benefit of this architecture is that it is difficult to mount an internal attack as there is no easy way to export information from the database to the outside world.

System Architecture

Not only must the system be safe against attacks from the Internet, but the overall system must have high availability, strong physical security, data integrity and security from Mother Nature.

High Availability

All systems are connected to Uninterruptible Power Supplies (UPS). Where needed, RAID disks are used.

Physical Security

There is physical security at SFNB’s data center and an even higher level of physical security in the actual machine room.

System Administration

System administration is on a 7x24 basis. All system administration is planned in advanced and with notification to all other system administrators of any scheduled activities. All administration of secure systems is logged and the logs independently checked on a regular basis. This is an expensive procedure, but a necessary one for any secure site.

Training

System administrators receive the necessary training to administer all systems.

Constant Monitoring

Various security related newsgroups and mailing lists are tracked. This is important because if there is a general security alert, SFNB can respond with information posted on its home page. This pro-active security awareness stance helps the company's reputation.

Authentication

There are several authentication problems with all Web based solutions.

The first problem is where should the authentication database be stored. Most Web servers provide an authentication capability implemented by storing username/encrypted passwords in an authentication database readable by the Web server. However this solution opens up security concerns for a secure site.

If the Web server must read the database, then if someone can exploit a hole in the Web server (despite all their claims, most Web servers have had some security problems in their short lifetime), the attacker also can read the authentication database. Admittedly, the database has encrypted passwords, but experience has shown that some passwords can be easily "cracked". If you are a bank, then even the fact that someone has a copy of your authentication database is enough for the public relations department to have the worst nightmares.

Other problems also occur if the authentication database is stored on the "outside". When a new account is opened, the new account name and initial password must be stored in the database. If this database is on the "outside", then there is some administrative interface running on the "outside". This was against the original security architecture which stated that no "trusted" code should be running on the "outside".

SFNB stores the authentication database on the Bank Database machine. This is a protected machine running on an inside network and allows for easier administration and much greater security.

Another authentication problem for Web servers is maintaining an authenticated state. The HyperText Transfer Protocol (HTTP) is supposedly stateless, however it does allow the passing of username/encrypted password as part of the protocol. Once someone has authenticated to the bank, they should only be allowed access to their account. This can be difficult to enforce as a CGI program cannot determine who the authenticator was.

To solve this authentication problem, Netscape "cookies" (see **http://www.netscape.com/newsref/std/cookie_spec.html** for more information) are used to indicate an authenticated state. Cookies are information that can be passed as part of the HTTP and are converted to environment variables by the Netscape Commerce Server.

New Customers

Much thought was given to the authentication scheme that would be used for customers. Several options were reviewed. Most were too expensive (smart cards) or too impractical (requiring customer to have a separate finger-print/retina reader). The common user/password combination was finally chosen as an interim step to browser client-side authentication.

New customers are assigned a random password. This is sent via regular mail after the customer’s address has been verified through a credit-checking agency. When this password is first used, the customer is forced to change the password and chooses their own password. Strict checks are made that the password is not a simple or easily-guessable password.

Maintaining Authenticated State

Once someone has authenticated, there is the problem of connecting the authenticator (the one who supplied the password) to the account he or she is authorized to access. This is solved by using the “cookies" described above.

Because the bank Common Gateway Interface (CGI) programs were the ones that generated the original “cookie”, the same programs can verify that the “cookie” belongs to the authorized bank customer. The bank maintains a database mapping a “cookie” to an account. Additional checks are made that the “cookie” expires and also is regenerated each time (to prevent replay attacks).

Encryption

The bank uses the Netscape Commerce Server’s SSL to provide encryption services.

Security Technology Employed

The overall architecture employs most of the security features found in a B1/CMW system.

Least Privilege

Least privilege is used in the trusted program that communicates between the “outside” and “inside”. The amount of trusted code in this program is very small and can be (has been) examined by inspection. This code is at the heart of the security of the system and is small enough, with enough documentation, to easily pass an A1 evaluation.

Mandatory Access Control (MAC)

MAC is used to provide the information separation to keep the “outside” and “inside” levels apart.

Discretionary Access Control (DAC)

The Netscape Commerce Server runs under a pseudo-user identity. This pseudo-user has read access to the files needed to run the Netscape Commerce Server and has write access to the Netscape log files. The pseudo-user has no other DAC rights on the system.

The Netscape Commerce Server is run in a *chroot*-ed environment providing further protection.

Audit

The system audits all appropriate information. The audit logs are reviewed on a frequent basis to determine any problems with the system.

System Integrity

The Bank Server uses system integrity to determine if any of the system files changed. System files can change either through system administration, or, in a worst case as part of a disk failure. The system integrity tools are run periodically by the Security Officer.

Potential Attacks

The following is a list of possible attacks, and how the system is designed to prevent the attack. SFNB does not divulge the type of attacks that may have been attempted.

IP Spoofing

The filtering router prevents IP spoofing.

User Name Spoofing

The authentication system prevents someone from pretending to be another user by requiring passwords to access the bank, transmitting all passwords encrypted, and using encrypted one-time “cookies” to maintain the authenticated state.

Attempts to Crack Authentication Database

Customer account information is stored on the database server which is protected behind a firewall and the HP/UX CMW. The database cannot be downloaded from the Internet.

Web Server Based Attacks

Attacks against the Netscape Commerce Server are thwarted because of the *chroot-ed* environment and because the “outside” processes cannot see anything on the “inside”. The firewall only allows mail to pass through and uses an SMTP filter. Each machine is minimally configured to only do its job, and nothing more.

Summary

The paper has presented the security architecture of SFNB, the world’s first on-line bank. The same architecture can be used for other financial institutions, or any company requiring a high level of security. The paper has also discussed some of the authentication issues associated with creating a secure Web server.

Since this work was done, Hewlett Packard acquired the secure web server technology and other assets from SecureWare and are marketing the secure web server technology as

“Virtual Vault”. The author left SecureWare to form his own security consulting company. SFNB went public in May 1996 and are buying the remainder of SecureWare.